

FIG. 1

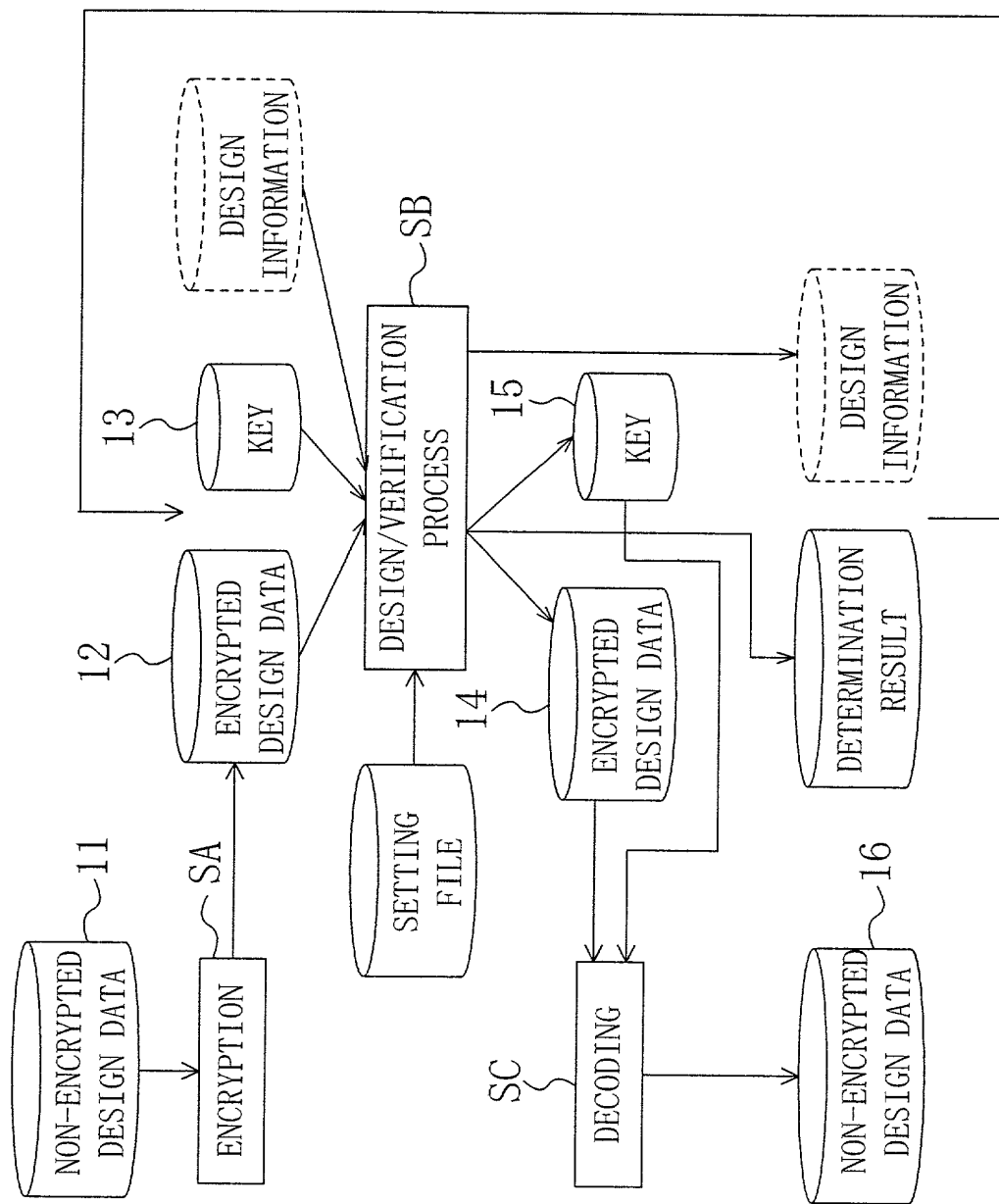


FIG. 2A

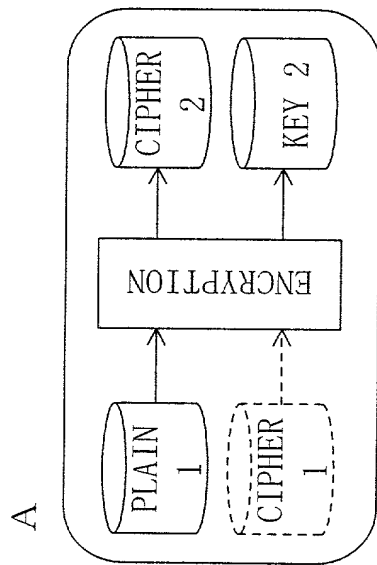


FIG. 2B

B 1 process of directly processing encrypted data

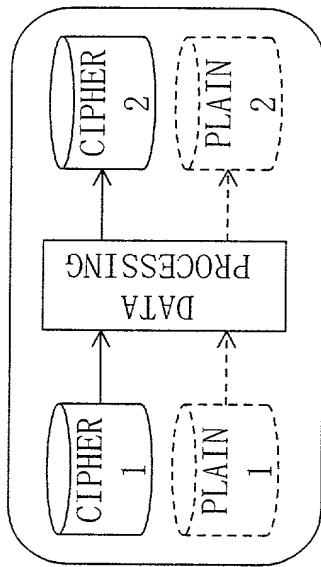


FIG. 2C

B 2 data conversion conducted with ciphers maintained

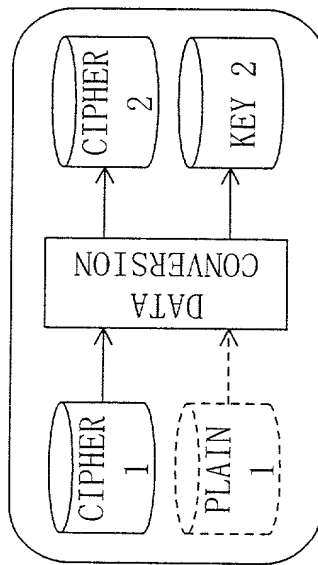
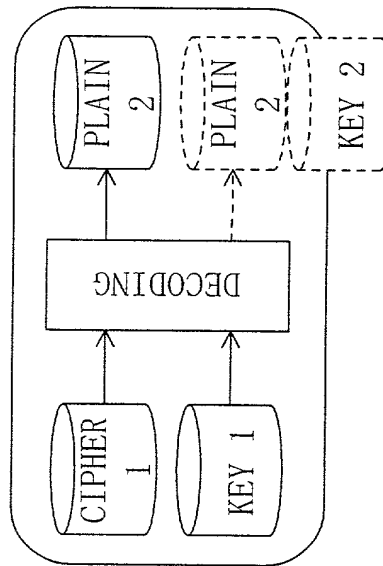


FIG. 2D

C



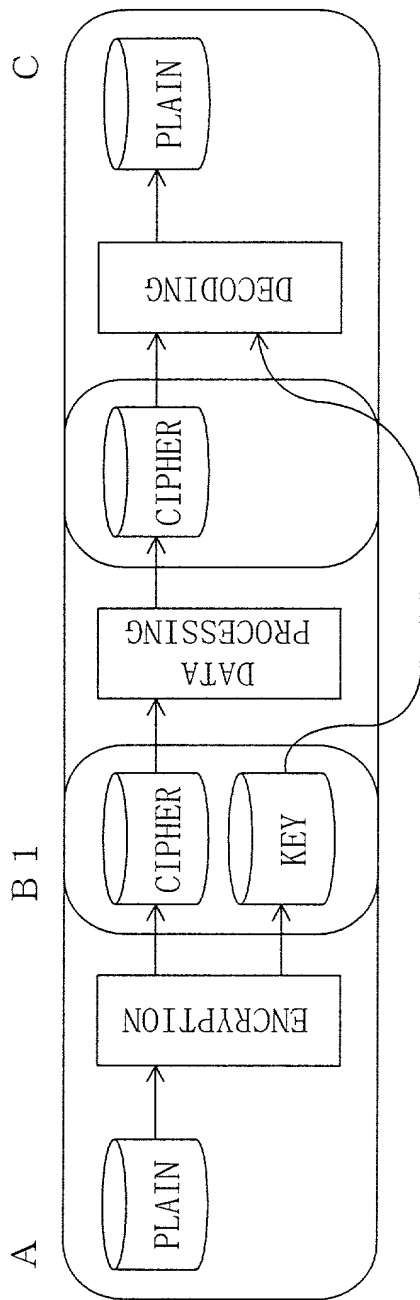


FIG. 3A

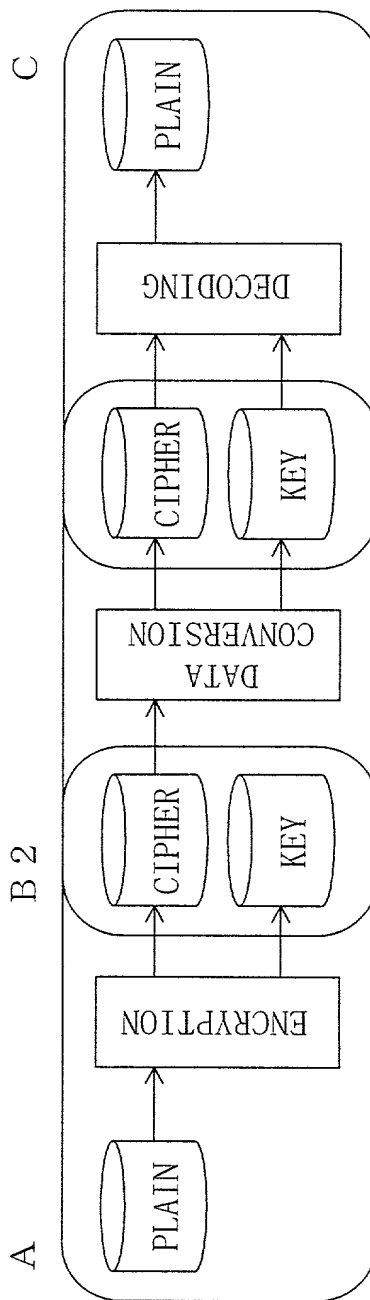
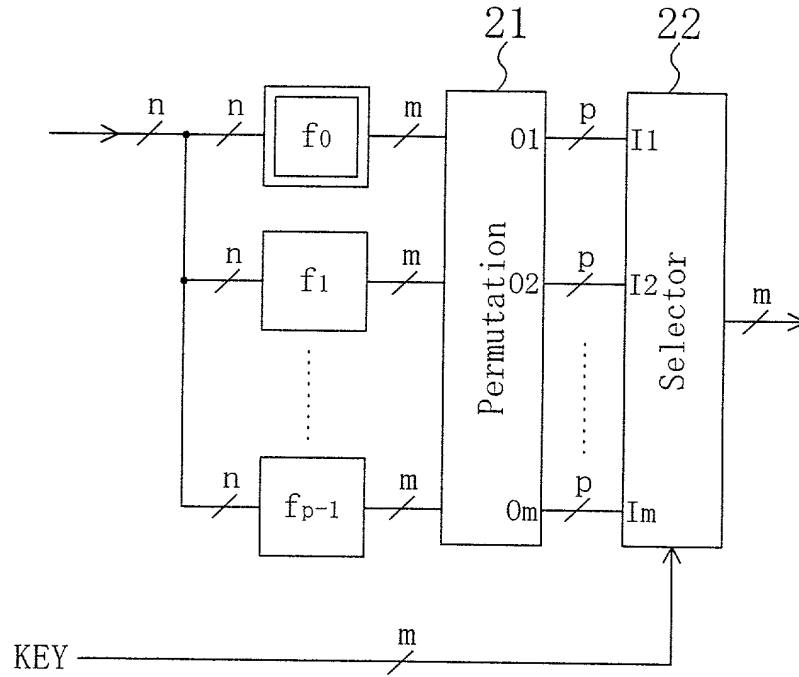


FIG. 3B

FIG. 4



FOBT 20" 0446/250

FIG. 5A
ORIGINAL CIRCUIT
f₀

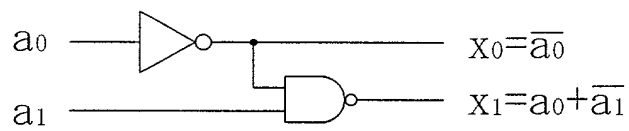


FIG. 5B
DUMMY CIRCUIT
f₁

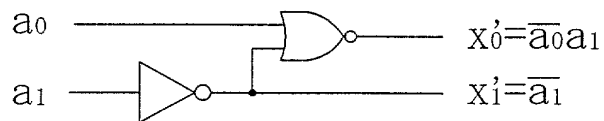


FIG. 5C

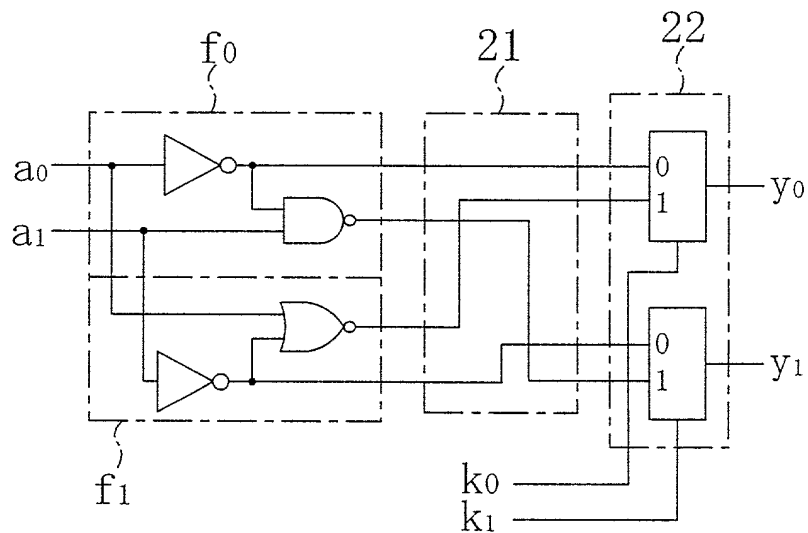
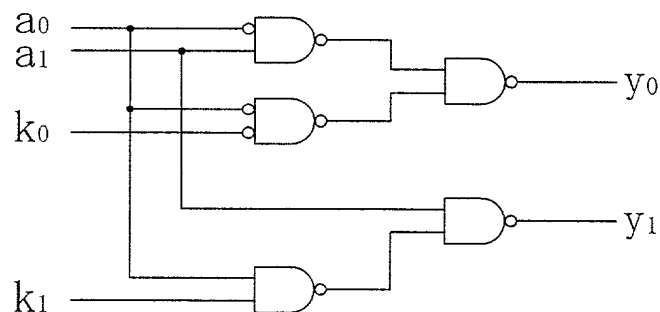


FIG. 5D



KEY = (0, 1)

FIG. 6

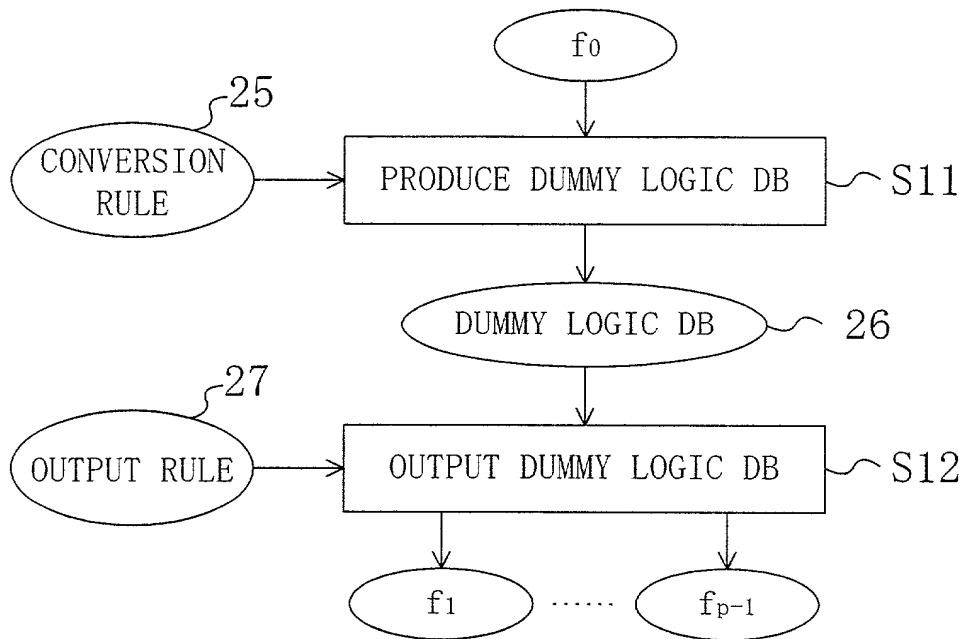


FIG. 7A

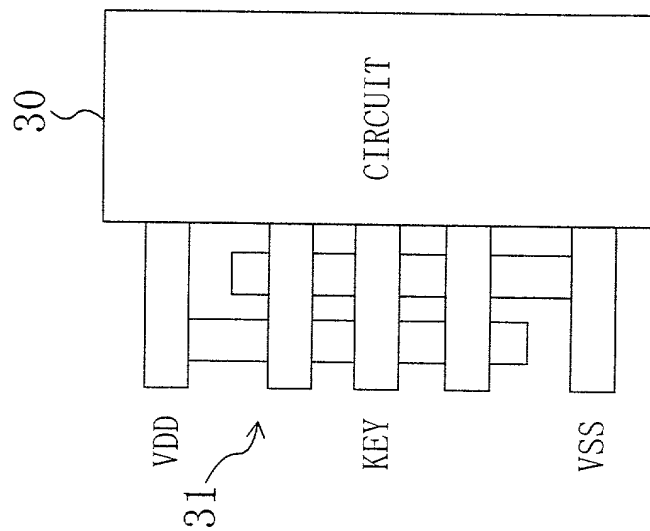


FIG. 7B

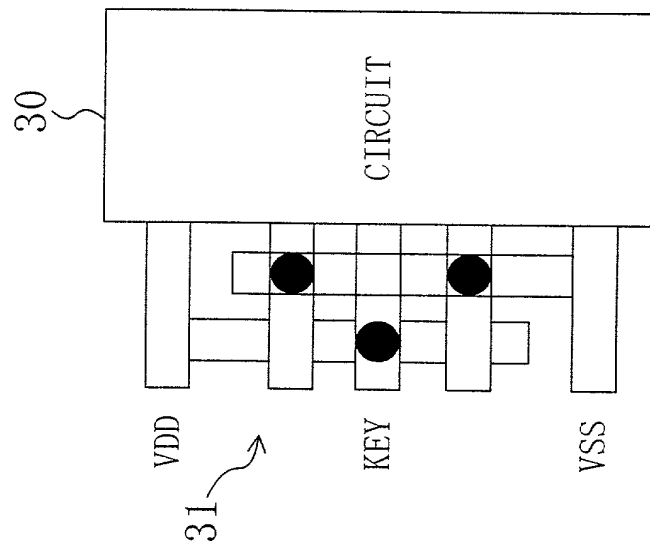
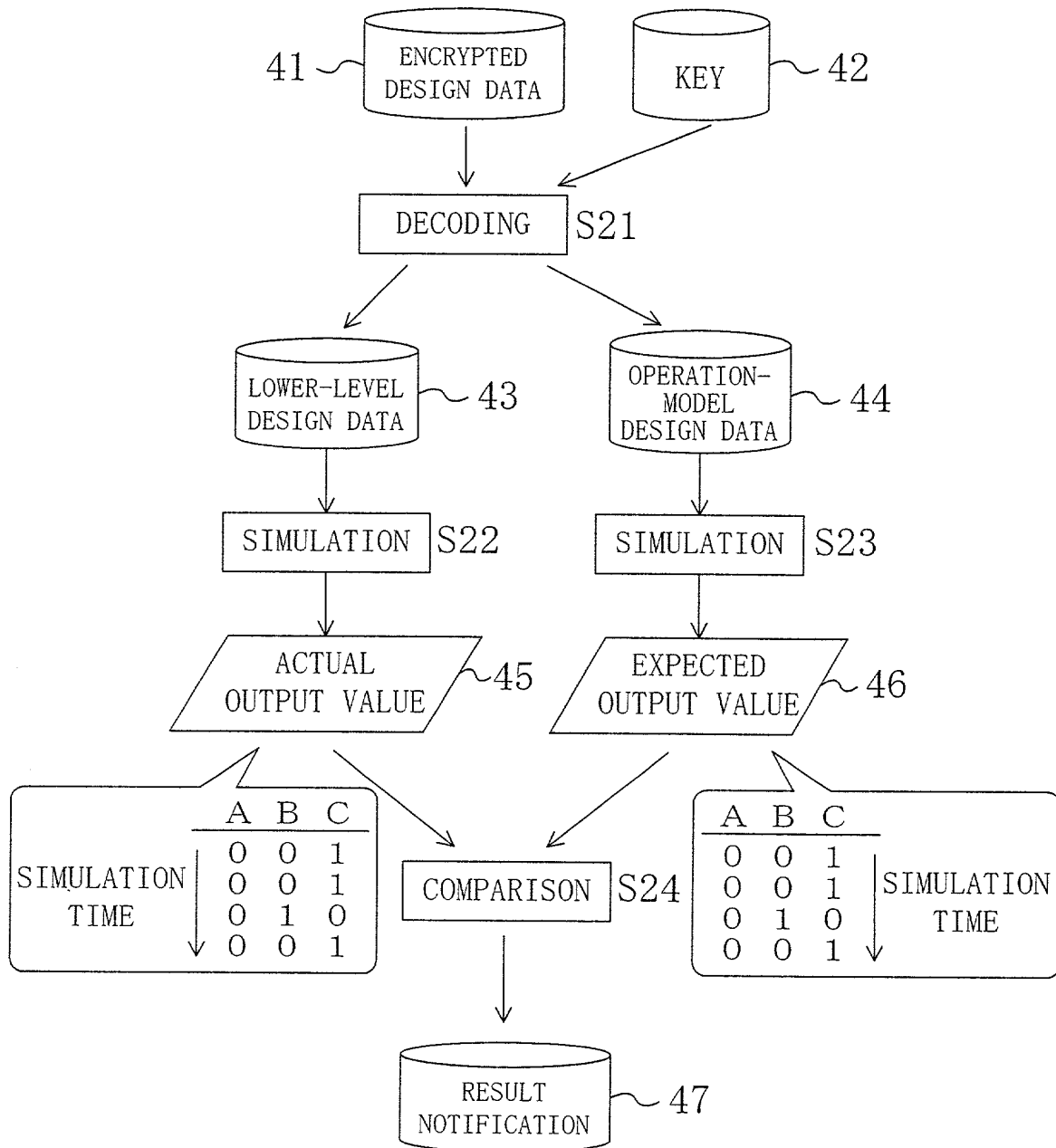


FIG. 8



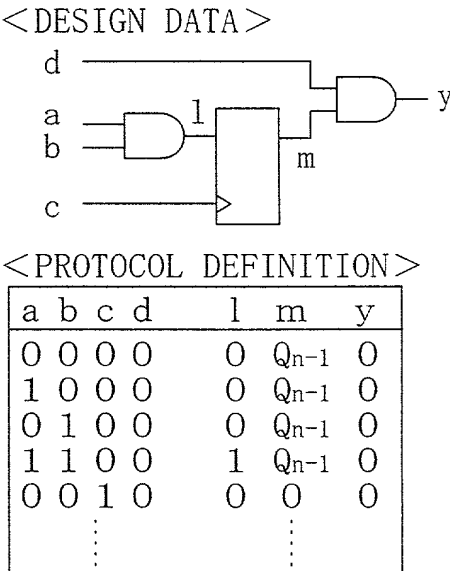
[illegible]

FIG. 10

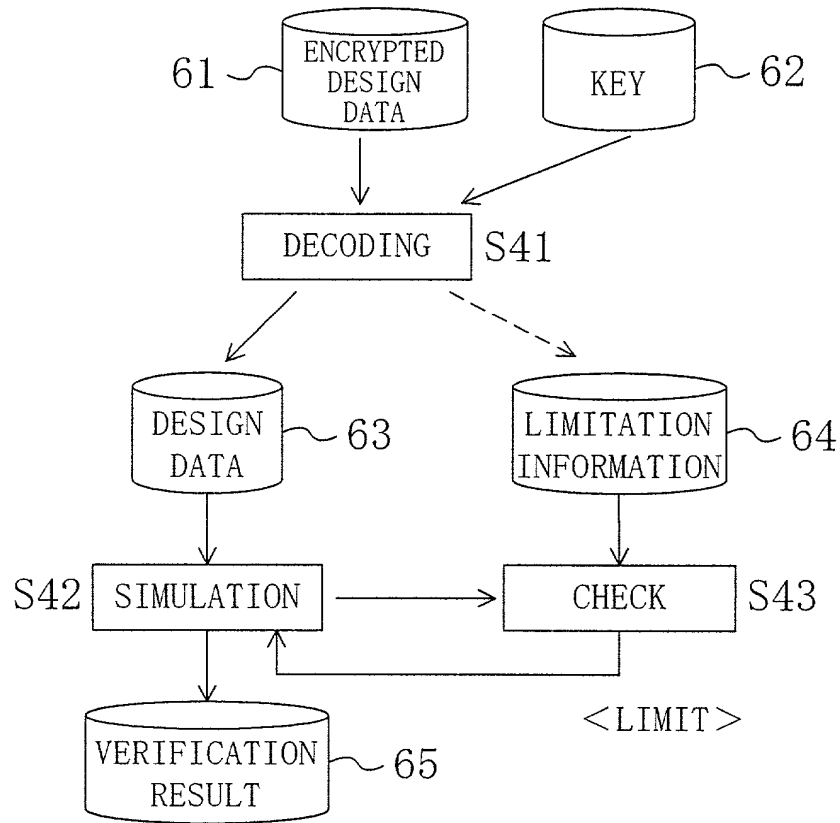


FIG. 11A

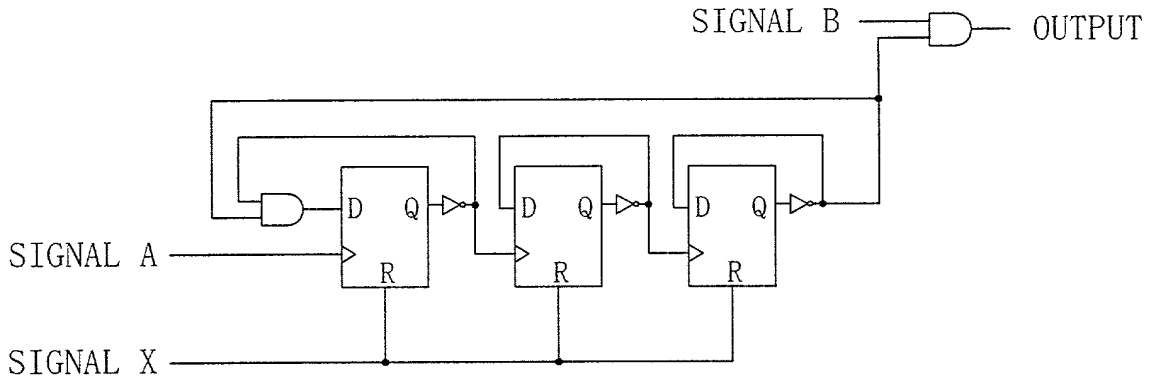


FIG. 11B

X	NUMBER OF TIMES A CHANGES	B	OUTPUT
0	1	0	0
		1	1
			} OK
0	2	0	0
		1	1
			} OK

0	7	0	0
		1	1
			} OK
0	8	0	0
		1	0
			} NG
0	9	0	0
		1	0
			} NG

105120-0445/250

FIG. 12A

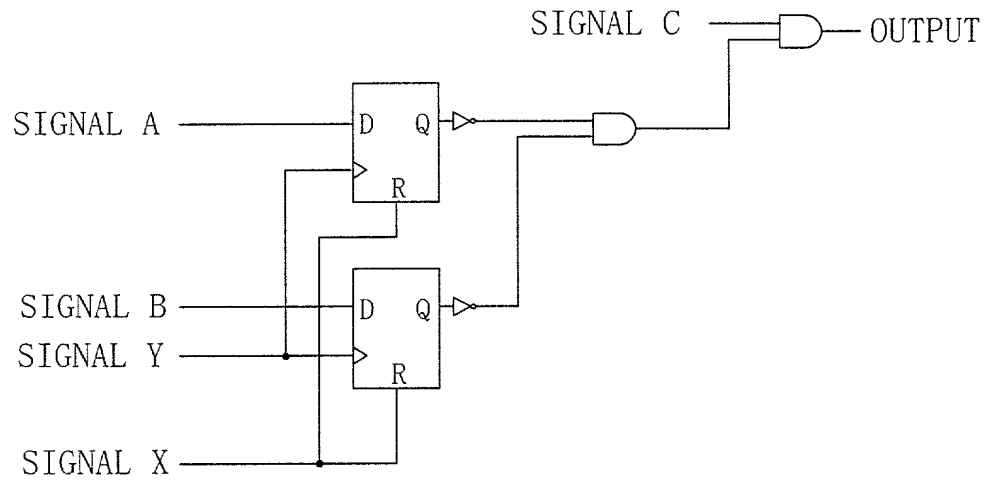


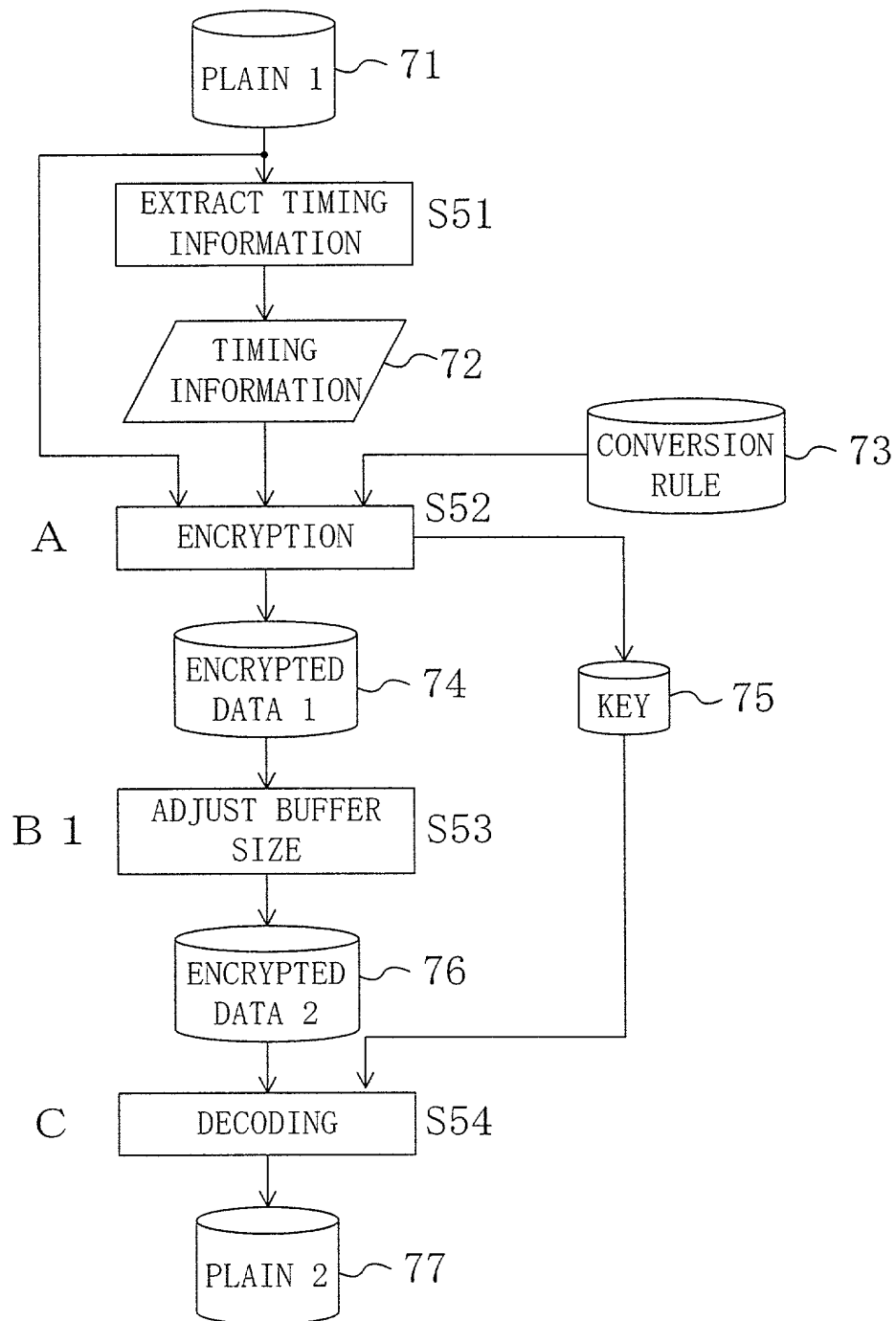
FIG. 12B

X	Y	A	B	C	OUTPUT
0	\uparrow	0	0	0	0
		0	0	1	1
<hr/>					
		0	1	0	0
		0	1	1	0
		1	0	0	0
		1	0	1	0
		1	1	0	0
		1	1	1	0

OK

NG

FIG. 13



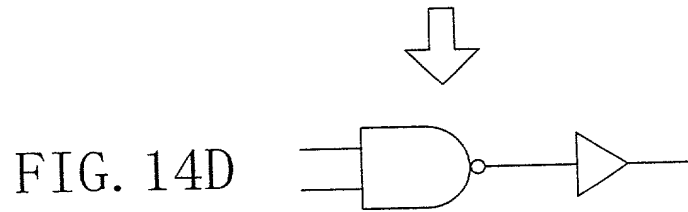
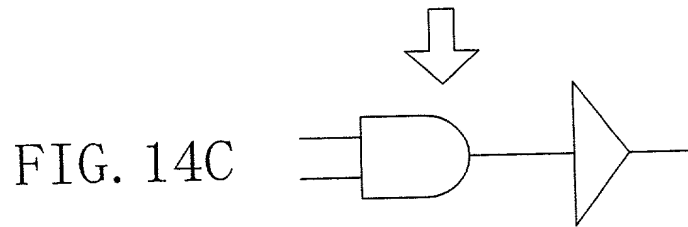
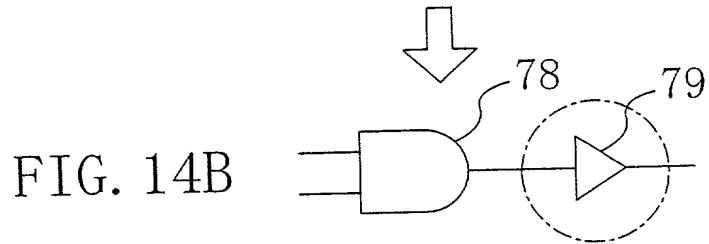
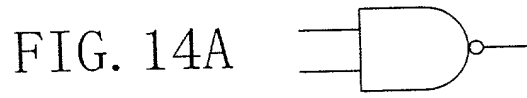
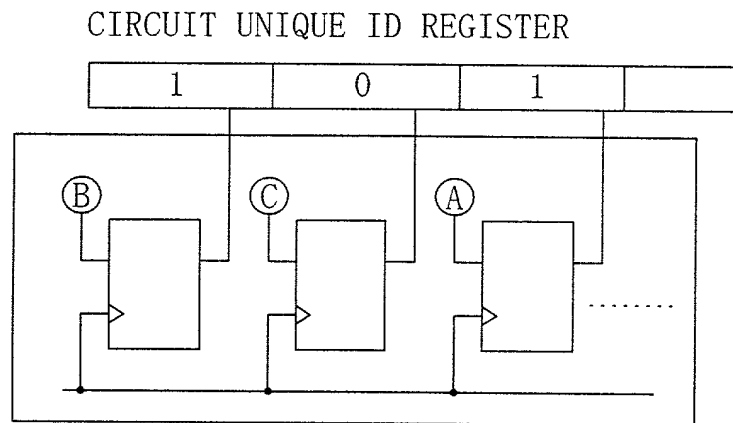


FIG. 15



$$\left. \begin{array}{l} A = 1 \\ B = 1 \\ C = 0 \end{array} \right\} \text{UNIQUE PARAMETER}$$

FIG. 16

